INTEGRATION GUIDE

Slack Integration

SHADOW AI
DISCOVERY · SECSTUDIO

Set up real-time Slack alerts for critical & high AI-security findings — Shadow AI Discovery & SecStudio.

1 · What this integration does

When enabled, every new **critical** and **high** finding posts a formatted message to a Slack channel of your choice — in real time, deduplicated — so the right people see high-severity AI risk the moment it's detected, with a link back to the finding in the dashboard.

> **Two products, one flow.** This works identically for **Shadow AI Discovery** and **SecStudio**, configured per-organization from the **Integrations** tab.

2 · Prerequisites

- A Slack workspace where you can add an app / incoming webhook.
- A target channel (e.g. `#ai-security`).
- Permission to create an **Incoming Webhook** (workspace admins may need to approve it).

3 · Create an incoming webhook

STEP 1 Go to `api.slack.com/apps` → **Create New App** → From scratch → pick your workspace.

STEP 2 Open **Incoming Webhooks** → toggle **Activate** → **Add New Webhook to Workspace**.

STEP 3 Choose the channel to post to and click **Allow**. Copy the webhook URL — it looks like `https://hooks.slack.com/services/T…/B…/…`.

4 · How to configure — in the dashboard (recommended)

STEP 1 Sign in as an **org-admin** → **Integrations**.

STEP 2 In the **Slack** card, paste the **Incoming webhook** URL and (optionally) the channel label for your own reference.

STEP 3 Tick **Send Slack alerts** → **Save**. The webhook is encrypted at rest and shown only as a masked placeholder afterwards.

STEP 4 Click **Send test message** — a test alert should appear in your channel within seconds.

5 · How to configure — self-hosted (environment)

```
SHADOW_AI_SLACK_WEBHOOK=https://hooks.slack.com/services/T00/B00/xxxx
# SecStudio:
SECSTUDIO_SLACK_WEBHOOK=https://hooks.slack.com/services/T00/B00/xxxx
```

Restart the service after setting it. Dashboard config takes precedence when its toggle is on; otherwise the environment value is used.

6 · The message template

Each alert posts a concise, pre-formatted message:

```
🚨 *[CRITICAL] Exposed AWS access key on finance-laptop-07*
Host: finance-laptop-07 · Score 95
A live AWS key was found in a committed file and is reachable.
*Fix:* Rotate the key and purge it from history.
```

Severity sets the icon (🚨 critical, ⚠️ high). The message is intentionally compact; the full evidence, compliance mapping and history live behind the dashboard link. To route different severities or teams to different channels, create multiple webhooks (roadmap: per-severity channel routing).

7 · Scope, limits & security

> **Treat the webhook like a password.** Anyone with the URL can post to that channel. It is encrypted at rest here and never returned to the browser. Revoke and re-issue it from the Slack app page if it leaks.

- Only **critical** and **high** findings post to Slack; medium/low do not.
- Messages are deduplicated — one post per finding.
- Only the summary is sent to Slack; detailed evidence stays in the dashboard.

8 · Troubleshooting

SYMPTOM	FIX
Test says `no_service / 404`	Webhook URL is wrong or was revoked — regenerate it.
`channel_not_found`	The channel the webhook was bound to was archived — create a new webhook.
Nothing arrives, no error	Confirm the **Send Slack alerts** toggle is on and there are actual new critical/high findings.